Fly-By-Wireless for Next Generation Aircraft: Challenges and Potential solutions

Dinh-Khanh Dang, Ahlem Mifdaoui
University of Toulouse-ISAE
dinh-khanh.dang@isae.fr, ahlem.mifdaoui@isae.fr

Thierry Gayraud
University of Toulouse-UPS / CNRS-LAAS
gayraud@laas.fr

Abstract—"Fly-By-Wireless" paradigm based on wireless connectivity in aircraft has the potential to improve efficiency and flexibility, while reducing weight, fuel consumption and maintenance costs. In this paper, first, the opportunities and challenges for wireless technologies in safety-critical avionics context are discussed. Then, the assessment of such technologies versus avionics requirements is provided in order to select the most appropriate one for a wireless aircraft application. As a result, the design of a Wireless Avionics Network based on Ultra WideBand technology is investigated, considering the issues of determinism, reliability and security.

Keywords-Time-critical, avionics network, fly-by-wireless, UWB, determinism, reliability, security.

I. Context and Related Work

The complexity of avionics communication architecture is increasing inherently due to the growing number of interconnected subsystems and the expansion of exchanged data quantity. To follow this trend, the current architecture of new generation aircraft like the A380, A400M or A350 consists of a high data rate backbone network based on the AFDX (Avionics Full Duplex Switched Ethernet) [1] to interconnect the critical subsystems. Then, each specific avionics subsystem could be directly connected to its associated sensors/actuators network based on low rate data bus like ARINC429 [2] and CAN [3]. Although this architecture fulfills the main avionics requirements, it also inherits weight and integration costs due to the significant quantity of wires and connectors. For instance, the wiring-related costs during fabrication and installation are estimated at $2000 per kilogram, which leads to a total cost ranging from $14 Million for an aircraft like A320 to $50 Million for one like B787 [4]. The new generation aircraft A380 in particular contains 500 km of cables which is one of the main reasons for production delays and cost overruns, estimated at $2 billion [4]. In addition to the cost issue, avionics interconnects are still subject to structural failure and fire hazard which decrease reliability and ramify the maintenance.

To cope with these arising issues, cable-less avionics implementation will clearly improve the efficiency and reliability of aircraft, while reducing integration, fuel consumption and maintenance costs. Therefore, "Fly-By-Wireless" paradigm based on wireless connectivity is proposed in this paper to decrease the weight and complexity of wiring.

Nowadays, wireless technology becomes one of the most cost effective solution thanks to its ubiquity, simplicity and maturity and it has been recently implemented for many real time applications such as wireless sensors network [5] and wireless industrial networks [6]. However, many interesting challenges still need to be handled due to its non deterministic behavior and its sensitivity to interference and jamming. These features could make it inadequate to deliver the hard real time communications required by aerospace applications. In this specific area, there are some recent works for unmanned aerial vehicle (UAV) [7] and some proposed solutions for aircraft that could be classified in accordance with the criticality level and the set of requirements to fulfill.
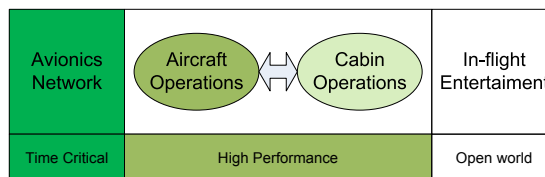

Fig. 1. Avionics Data and Communication Network

As shown in figure 1, the Avionics Data and Communication Network (ADCN) consists of mainly three types of systems where time critical is the highest criticality level while high performance and open world correspond to the medium and lowest levels, respectively. For open world and high performance systems, one of the main constraints is to increase the bandwidth utilization, whereas the predictable behavior and deadlines guarantee are not necessarily the primary design concern. In the area of open world systems, in [8], the authors have performed some simulations and experiments on using standard wireless technologies for the In Flight Entertainment Network (IFE). The obtained results for an heterogeneous architecture based on Ethernet and Wireless USB technologies are promising in terms of QoS. For the high performance systems, [9] has investigated Ultra WideBand technology for in-cabin communication with optimized resource allocation, and average communication latencies have been achieved using simulation. In addition, [10] surveys and presents several recent works on using wireless sensor networks for aircraft control and health monitoring.

Unlike existing approaches in this area, this paper focuses on a specific solution based on standard wireless technologies

for time critical systems to fulfill the hard real time and safety requirements. Our main contributions in this paper are three folds. First, the main arising challenges when using wireless technologies in avionics context are identified. Then, an assessment of Commercial Off-The-Shelf (COTS) wireless technologies versus avionics requirements is conducted to select the most accurate one for critical avionics applications. Third, the design of a Wireless Avionics Network (WAN) based on Ultra WideBand technology is investigated, considering the issues of timeliness, reliability and security.

The remainder of the paper is organized as follows. In the next section, the current avionics communication architecture and its main requirements are described, then the main challenges to replace this latter by wireless technology are presented. In Section III, the most common wireless technologies satisfying most of the avionics requirements are described and their pros and cons versus avionics requirements are discussed. Section IV presents the proposed WAN design where the considered architecture, the MAC protocol and reliability mechanisms are detailed. Section V concludes the paper.

II. PROBLEM STATEMENT

In this section, we first present the current Avionics Network (AN) based on wired technologies and its main requirements. Then, we describe the main benefits and risks of using wireless connectivity in avionics context and detail the arising issues of an alternative WAN.
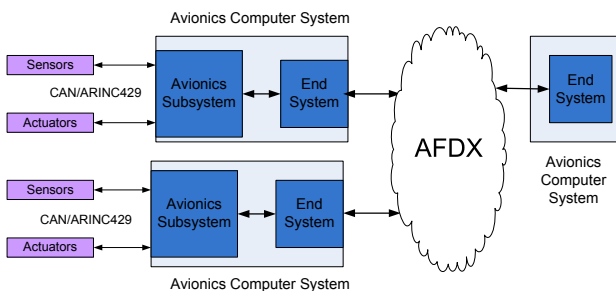
A. Current Avionics Network

Fig. 2. Current Avionics Network

As shown in figure 2, the current avionics network consists of a backbone network AFDX to interconnect the avionics End Systems; and some specific subsystems admit dedicated sensors/actuators network based on CAN or ARINC429 buses. The former is responsible for flight control, cockpit, engines and landing gears. The time critical subsystems, interconnected to the backbone network, are geographically concentrated in two avionics bays, the main and the upper, at the head of the aircraft as shown in figure 3.

AFDX: The AFDX [1] network is based on Full Duplex Switched Ethernet protocol at 100 Mbps, successfully
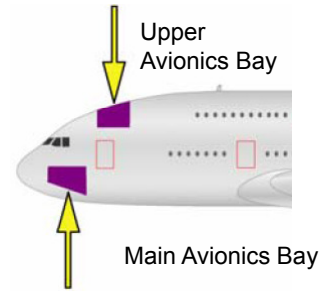

Fig. 3. Avionics bays

integrated into new generation civil aircraft like the Airbus A380. This technology succeeds to support the important amount of exchanged data due to policing mechanisms added in switches and the Virtual Link (VL) concept. This latter gives a way to reserve a guaranteed bandwidth to each traffic flow. The VL represents a multicast communication which originates at a single end-system and delivers packets to a fixed set of end-systems. Each VL is characterized by: (i) BAG (Bandwidth Allocation Gap), ranging in powers of 2 from 1 to 128 milliseconds, which represents the minimal inter-arrival time between two consecutive frames; (ii) MFS (Maximal Frame Size), ranging from 64 to 1518 bytes, which represents the size of the largest frame that can be sent during each BAG.

CAN: The CAN bus [3] is a 1 Mbps data bus that operates according to an event-triggered paradigm where messages are transmitted using a priority-based access mechanism. CAN bus works by using a producer/consumer communication scheme based on unique identifier per message type. The CAN messages are broadcast on the bus, then each CAN equipment will filter the consumed data based on the CAN identifier. The collisions on the bus are resolved following a CSMA/CR protocol (Carrier Sense Multiple Access/ Collision Resolution) thanks to the bit arbitration method. The CAN frame consists of a payload up to 8 bytes and an overhead of 6 bytes due to the different headers and bit stuffing mechanism.

ARINC429: The ARINC429 [2] is a 100 Kbps data bus with point-to-point protocol. It is a mono-transmitter-multi-receivers data bus with unidirectional communication which provides high reliability at the cost of wire weight and limited data rate.

In order to replace the Time-Critical Avionics Network, the following requirements have to be considered:

- Hard real time and Determinism: AN must behave in a predictable manner where the timeliness of data has to be guaranteed for determinism concerns. Therefore, information transmission latencies have to be bounded and respect the deadlines constraints;
- Reliability and Availability: in terms of fault tolerance, AN has a high criticality level and the required probabil-

ity of failure is less than 10^{-9} per flight hour. Therefore, AN needs to implement the necessary fault detection and recovery mechanisms to satisfy this condition. Concerning maintainability, the lifetime of an avionics system is about 20 to 30 years which needs an easy incremental design process for adding functions along this duration. Hence, the used technologies for AN needs to be mature and have long-term support;

- Security: in [11], the authors point out the security requirements for AN which has to guarantee: (i) data confidentiality to ensure the privacy of end-users and keep the information secret by preventing passive eavesdropping from unauthorized users; (ii) data integrity to guarantee that the message from sender is original and not altered in transit by an adversary; (iii) authentication to prevent the unauthorized access to the network;
- Electromagnetic Compatibility: the avionics network has to cope with a harsh physical environment with important vibration, temperature variation and humidity. In addition, it must be able to work normally with the presence of intense radio frequency noise and should not cause interference to other aircraft systems.

The work presented in this paper is mainly focused on the replacement of the current backbone avionics network with wireless network. Peripheral sensors/ actuators networks are not considered in this paper and will be analyzed in future work.

B. Wireless Avionics Network

In this section, we propose to both discuss the benefits and risks of implementing wireless technologies for safety critical avionics network, and to identify the main research locks.

Nowadays, wireless technology has progressed and introducing this concept for avionics has become feasible but also advisable for the following reasons: first, a Wireless Avionics Network (WAN) will allow an inherent weight reduction and an increase of system's flexibility and efficiency through less fuel consumption and better flight autonomy; second, eliminating the wiring-aging-related problems shall enhance the system scalability and safety thanks to simpler fault allocation process and less fire hazards; third, cable-less avionics implementation will inherently reduce the costs not only during design, production and development process but also for maintenance and overhaul.

Currently, there is a new trend to use commercial-off-the-shelf (COTS) technology rather than designing a dedicated solution to reduce the development costs. However, the problem with COTS is reconciling the different requirements between commercial and safety-critical applications. For wireless technologies, the main concerns are related to the system's susceptibility against ElectroMagnetic Interferences (EMI). This is mainly due to natural phenomena or man-made events that could be internal or external to the plane, e.g. Portable Electronic Devices (PED), satellite communications or Radio Navigation. This results in both data rate and QoS degradation or even network collapse. Furthermore, there is system security

issue due to the access and manipulation of sent information (Man-in-the-Middle) and denial of service (DoS) attacks [12].

Hence, as one can notice there is a trade-off to handle between efficiency and dependability when implementing wireless technologies for safety-critical applications. We identify herein the main arising issues to design a new WAN.

Assessment of Wireless Technologies: In order to derive a specification for a WAN, one must begin by analyzing the characteristics of the current AN. Then, with an understanding of these requirements, suitable COTS wireless technologies could be identified in order to select the most efficient one for safety-critical avionics applications.

WAN design: The choice of the wireless technology for the future WAN is one of the first issue to fix before considering other important aspects concerning for instance the network architecture to implement and the main communication protocols to define.

- *Network Architecture*: replacing the current avionics interconnections by wireless connections arises many questions concerning the end systems clustering and topology but also the introduced mechanisms to avoid interferences.
- *MAC protocol*: the choice of the MAC protocol will directly impact the communication timeliness and predictability which are of the utmost importance for safety-critical avionics systems. Hence, the MAC protocol should be well defined to guarantee this requirement.
- *Reliability Mechanisms*: for safety-critical avionics network, the probability of failure should not be greater than 10^{-9} per flight hour. Hence, any wireless system should meet this requirement. The arising question here concerns the feasibility of a full wireless avionics network or the necessity of backup system. Furthermore, the avionics communications are mainly multicast which needs the integration of an enhanced acknowledgment and retransmission mechanism to reduce the communication overhead. The reliability mechanisms should be well selected to achieve these requirements.
- *Security Mechanisms*: Security is one of the most important criteria to achieve for safety-critical avionics applications. Therefore, WAN has to provide authentication, data encryption and integration to avoid "man-in-the-middle" or DoS attacks.

Schedulability Analysis: For avionics embedded applications, it is essential that the communication network fulfills certification requirements, e.g. predictable behavior under hard real time constraints and temporal deadlines guarantees. However, the use of wireless technologies may increase the communication latencies due to transmission errors; hence, real time constraints have to be verified under error prone environment. In order to deal with the worst case performance analysis of such network, an appropriate schedulability analysis has to be considered. This issue will be handled in future

work.

III. Wireless technologies versus avionics requirements

In this section, the main specifications for Wireless Avionics Network (WAN) are detailed. Then, the most common wireless technologies that satisfy the identified specifications are described and their pros and cons versus the avionics requirements are discussed.

A. Specifications of a Wireless Avionics Network

In order to replace the current AN with a wireless network, the requirements described below have to be guaranteed and the specific conditions of avionics context should be integrated. The main identified specifications are the following:

- The offered data rate by the current backbone network is about 100 Mbps. The new technology must provide the higher capacity to meet the scalability of AN during an aircraft's lifetime (20-30 years). Hence, the considered wireless technology should at least offer this required data rate 100 Mbps.
- The range for each avionics bay is short (4-6 meters). Distance between 2 different avionics bays is 6 meters but can be extendable;
- Currently, there are 50 to 80 end-systems connected to the backbone network. Hence, the selected technology for this kind of communication should be able to connect at least this number of nodes;
- The current avionics end-systems are considered as complex equipments implementing many avionics functions that have to be powered all the time and their positions are fixed. Hence, the problems related to energy consumption and mobility are not considered as important performance objectives in the avionics context;
- The AFDX traffic is transmitted within Virtual Links which represent multicast communication pattern, originated at a single source and delivered to a fixed set of destinations. Hence, the communication pattern should be any and multicast for the WAN with peer-to-peer topology;
- The avionics data is time-constrained and has a high safety level. Hence, the determinism and particularly the predictability of end-to-end delays and the reliability of communication are of the utmost importance. These requirements imply contention free access methods with accurate reliability mechanisms.

The main identified characteristics of physical and MAC layers for WAN are summarized in table I.

B. Wireless technologies standards for backbone network

The most common wireless technologies that satisfy the required data rate for backbone network are described in this section.

TABLE I
PHYSICAL AND MAC LAYERS CHARACTERISTICS

		Backbone network
PHY Layer	Per link data rate	≥ 100Mbps
	Subnetwork size	$50 - 80$ nodes
	Range (meters)	$4 - 6$ for each avionic bay & ≥ 6 for 2 avionic bays
	Topology	peer-to-peer
	Network pattern	any, multicast
MAC Layer	Mechanism	Contention free access
	Delay	End-to-end delay guarantee
	Reliability	End-to-end reliability guarantee
	Energy	No specific limitations on power consumption

1) IEEE 802.11: Among several variants of IEEE 802.11, only the standard IEEE 802.11n [13] can provide the sufficient data rate to replace the current avionics backbone network. The IEEE 802.11n operates at 2.4 and 5 GHz bands with two bandwidth options, 20 MHz or 40 MHz. This standard uses multi-transmit-multi-receive antenna (MIMO) to achieve the maximum data rate 600 Mbps in range of 30 meters for indoor environment. IEEE 802.11n MAC is based on CSMA/CA mechanism, and integrates a contention based DCF protocol (Distributed Coordination Function) for ad-hoc mode and contention free PCF protocol (Point Coordination Function) for infra-structure mode.

At PHY layer, IEEE 802.11n implements the Forward Error Code (FEC) and Low-density parity-check (LDPC) for controlling errors and improving reliability. At MAC layer, IEEE 802.11n uses Automatic Retransmission ReQuest (ARQ) with different kinds of acknowledgement, i.e. immediate-ACK, delay-ACK and block-ACK.

For security concerns, the IEEE 802.11n adopts the same mechanisms than IEEE 802.11i based on three data confidentiality protocols: Wired Equivalent Privacy (WEP), Temporal Key Integrity Protocol (TKIP), and Counter-mode/CBC-MAC Protocol (CCMP). The former uses weak RC4 stream cipher while the two others use Advanced Encryption Standard (AES) algorithm which is more secure against brute-force attacks. Furthermore, TKIP and CCMP protocols provide Message Integration Code (MIC) and the authentication is enhanced due to Extensible Authentication Protocol (EAP).

While IEEE 802.11n can provide the sufficient data rate and the required reliability and security mechanisms for avionics applications, there are still less researches focusing on ad-hoc reliable multicast using MIMO technique. In addition, CSMA/CA cannot provide the determinism for MAC layer with ad-hoc mode. Moreover, this standard would be inherently sensitive to interference caused by IFE systems and common devices like laptop or PDA which are operating at the same frequencies bands. These aspects represent a real limitation to use the IEEE 802.11n standard for the avionics backbone network where communication pattern is any and predictability is required.

2) ECMA-368: ECMA-368 is a standard for High Rate Ultra WideBand (HR-UWB) technology within a short range operation [14]. This standard operates at large frequency band from 3.1 GHz to 10.6 GHz which is divided into 14 non-overlapping 528 MHz-Bands. Nowadays, three bands are still

not used and are common to all over the world (bands 9, 10 and 11). This fact is very interesting for avionics applications as they need universal frequency bands to avoid reconfiguration during the flight and reduce the interference risks with common devices. ECMA-368 can support data rate of 110 Mbps, 200Mbps and 480Mbps in a range of 10m, 6m and 2m, respectively.

ECMA-368 supports the peer-to-peer topology and two MAC protocols: Prioritized Contention Access (PCA) and Distributed Reservation Protocol (DRP). The former is a contention-based protocol with prioritized Quality of Service (QoS), whereas the latter is TDMA-based protocol to guarantee a contention-free access.

In terms of reliability, ECMA-368 supports FEC convolutional code with different coding rates at PHY layer and retransmission mechanisms with Immediate Acknowledgement (Imm-ACK) and Block Acknowledgement (B-ACK) at MAC layer.

This standard integrates strong security mechanisms. For data encryption, it uses AES algorithm with Pairwise Transient Key (PTK) for unicast communications, and Group Transient Key (GTK) for multicast and broadcast communications. Furthermore, like IEEE 802.11n, integrity is guaranteed with MIC and the authentication is based on 4-way handshake.

Since spatial containment and using the different frequency bands from ISM 2.4 GHz, ECMA-368 is less sensitive than 802.11n to interference from other common devices. In addition, ECMA-368 with low energy and low range emission is more secured than 802.11n for "man-in-the-middle" attack since it requires of the attackers to be very close to the end-systems. Hence, due to its high data rate, security mechanism and deterministic MAC protocol with peer-to-peer topology, ECMA-368 represents a good candidate to replace the current avionics backbone network.

3) IEEE 802.15.3c: One of the recent wireless technologies is 60 GHz technology, standardized as IEEE 802.15.3c. This latter aims to provide Gigabit wireless communication under 60 GHz frequency band [15] with 7 GHz bandwidth. Due to severe attenuation by oxygen absorption, 60 GHz has to be based on directional antennas with Light-of-Sight (LoS) condition to achieve the range of 10m with data rate up to 3 Gbps. This technology is still under development with several options for modulation technique and MAC protocol, where TDMA could be one of the optional implementations.

In terms of reliability, this technology integrates the same aggregation data and B-ACK mechanisms as IEEE 802.11n and it introduces some improvements due to the retransmissions of individual MSDUs and different coding rates for aggregated MSDUs.

Because of its LoS requirements and its immaturity, this technology is considered as inadequate to replace the current avionics backbone network.

C. Selected wireless technologies

The main characteristics of the described wireless technologies are summarized in table II. The comparison of these three

TABLE II
WIRELESS TECHNOLOGIES PARAMETERS

Standard	802.11n	HR-UWB	60 GHz
Max Range (m)	30	10	10
Frequency bands	2.4, 5GHz	3.1-10.6 GHz	60GHz
Bandwidth	20/40Mhz	500MHz-7.5GHz	5-7GHz
Non-overlap channels	3	14	1
Modulation Technique	64QAM	QPSK	QPSK, 64QAM
Spread Spectrum	OFDM	MB-OFDM	OFDM or SC-FDE
LoS requirement	No	No	Yes
Max data rate (Mbps)	600	110 (10m)/ 200(6m)/480(2m)	3000
Encryption	RC4, AES	AES	NA
Topology	ad-hoc, infrastructure	peer-to-peer	NA
MAC protocol	CSMA/CA DCF, PCF	TDMA or CSMA/CA HCF	TDMA

TABLE III
WIRELESS TECHNOLOGIES VS AVIONICS REQUIREMENTS

	802.11n	ECMA-368	IEEE 802.15.3c
Determinism	PCF (Yes), DCF (No)	TDMA (Yes), PCA (No)	Yes
Reliability	Medium	Medium	Medium
Security	High	High	N.A
EMC Susceptibility	High	Low	Low

technologies in terms of avionics requirements is shown in table III. From this analysis, ECMA-368 is considered the most accurate one to replace the avionics backbone network because of its high data rate, deterministic MAC protocol and high security mechanism. However, there still are some challenging issues to integrate this technology for avionics applications.

The rest of the paper will be focused on the design of the Wireless Avionics Network based on this technology.

IV. WIRELESS AVIONICS NETWORK DESIGN

In this section, we present first the considered architecture for the proposed Wireless Avionics Network. Then, we detail the selected MAC protocol to enhance the communications predictability and determinism. Finally, the selected reliability mechanisms to fulfill the avionics requirements are described.

A. Hybrid Architecture ECMA-368/ Switched Ethernet

As described in table I, the current backbone network consists of maximum 80 end-systems. They are concentrated in two avionics bays at the head of the aircraft, as shown in figure 3. Furthermore, the area of each avionics bay is less than the area of a 6m-diameter circle.

Since there are more end-systems in the main bay and three free frequency bands (9, 10 and 11) of ECMA-368 standard that could be reserved for avionics applications, our proposed architecture is based on three clusters of end-systems (2 clusters in the main bay, 1 cluster in the upper bay) where each cluster is assigned a reserved band to avoid interference with the two others. Hence, the achieved rate within each cluster in a range of 6 meters is about 200 Mbps. Furthermore, each cluster has a peer-to-peer topology which guarantees single hop intra-cluster communications.

The inter-cluster communication is handled by specific gateways and the communication patterns between gateways could be unicast, multicast or broadcast. Since the distance between the main and upper avionic bays is about 6 meters (see figure 3), two main solutions could be considered for the gateways interconnection: wireless or wired interconnection.

With wireless interconnections between the gateways, the end-to-end delays can inherently increase due to the required contention-free access mechanism and half-duplex communication. Moreover, this architecture should be more sensitive to interference and reduce system scalability. In fact, the addition of new avionics bays in the middle or in the back of the aircraft will require many relaying nodes between the gateways. The offered rate in this case is about 200Mbps between two consecutive relaying nodes, but much smaller between the gateways. Hence, this solution is considered as inadequate for the inter-cluster communications within the avionics network.

In order to cope with the limitations of a full-wireless architecture, an hybrid architecture based on a Full Duplex Switched Ethernet at 1Gbps to interconnect the three clusters is considered as an interesting solution. As shown in figure 4, a central switch is used to connect the three gateways. Unlike the wireless interconnection where the gateways have to transmit their messages only during their exclusive slots, with the Full Duplex Switched Ethernet, each gateway can transmit immediately its messages to the switch, to be then relayed to the final destination(s). Hence, this characteristic allows high rate, deterministic and reliable communications. Furthermore, this hybrid architecture is more scalable since additional avionics bays in the middle or in the back of the plane can be easily interconnected. Given all these advantages, we consider the hybrid architecture to design the Wireless Avionics Network.
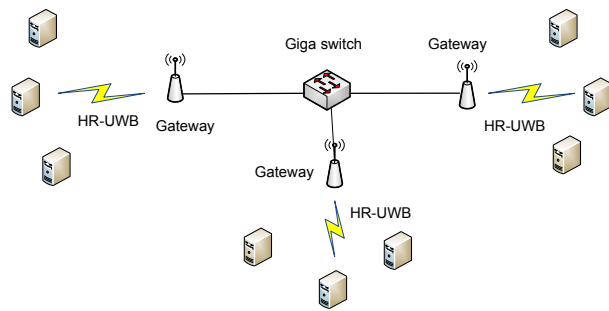

Fig. 4.   Proposed Avionics Network with hybrid architecture

It is worth to note that the gateways and the switch in this hybrid architecture have key functions. Each gateway has to convert the received ECMA-368 frames from any end-system in its associated cluster to Ethernet frames that will be transmitted to the Ethernet switch. Hence, to keep the end-to-end communication transparency, each gateway proceeds as follows: each received ECMA-368 packet from an end-system in the associated cluster is encapsulated in an Ethernet frame (which respects the minimal and maximal sizes) and then transmitted to the Ethernet switch; and each received Ethernet frame from the Ethernet switch is decapsulated to extract the ECMA-368 packet to be then transmitted to the final destination. ECMA-368 and Giga Ethernet frames are

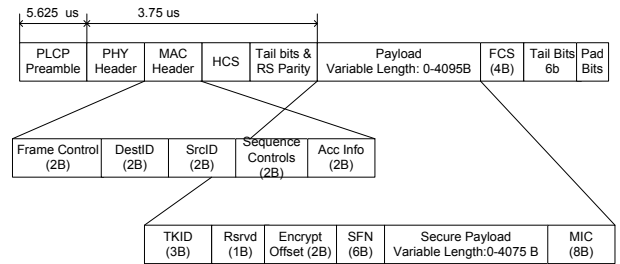described in figures 5 and 6:
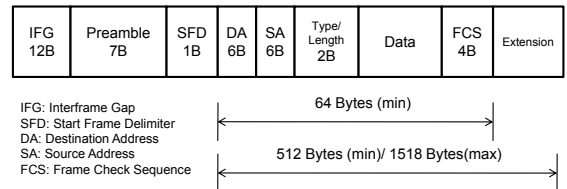

Fig. 5.   ECMA-368 Frame Structure

Fig. 6.   Ethernet frame structure

The Ethernet Switch is an active device that identifies the destination port of an incoming packet and relays it to the specific port. If multiple packets have the same destination port, buffers are used to solve the problem of collision. Ethernet switches can be identified by their switching technique and their scheduling policy. First, two types of switching techniques are currently implemented in Ethernet switches: *Cut Through* and *Store and Forward*. With the first, only the header of each packet is decoded to determine its destination port and the rest is forwarded without any error checking mechanism. With the latter, the switch waits until the complete reception of the packet and forwards it to the destination port if it is successfully verified. In our case, we choose the second switching technique for safety reasons since no corrupted packet will be forwarded. Then, the scheduling policy is used to forward packets at the switch output port. We consider the most widely implemented policy, First Come First Served (FCFS), where packets are served in their arrival order without taking into account of their temporal characteristics.

B. MAC Protocol Overview

As described in section III-B2, ECMA-368 supports two MAC protocols: PCA and DRP. The former is a contention based protocol with prioritized Quality of Service (QoS), whereas the latter is TDMA-based protocol to guarantee a contention-free access.

Since for avionics applications, it is essential to guarantee predictable behavior under hard real time constraints, DRP protocol seems more accurate than PCA one for this context. However, the slots allocation and the cycle duration must be carefully configured, since it must efficiently handle different types of traffic and guarantees different temporal constraints.

The following assumptions are considered for our proposal:

Off-line configuration: since all generated messages are known a priori, the slots allocation mechanism is configured off-line and it will be followed in a static manner by all the end-systems during the network deployment;

Slots and cycles durations: during each minor cycle, the allocated time slot for each end-system is fixed and has a defined duration that depends on its generated traffic. Hence, the time slots are not equally allocated to the different end-systems and the cycle duration could differ from one cluster to another;

Synchronization protocol: in order to implement an accurate TDMA protocol for time-critical avionics network, the precision's degree of the used synchronization protocol is of the utmost importance. For wired networks, many synchronization protocols were successfully implemented with a precision degree about few nanoseconds, and the most known one is the IEEE1588 protocol [16]. However, for wireless networks, achieving this tight precision's degree seems more complicated due to many variable factors during communication. A recent work [17] investigated the IEEE1558 performances for wireless sensor networks and the obtained precision is less than 200 nanoseconds. However, [17] cannot be applied directly to our context due to large number of exchanged messages for synchronization. [18] proposed an enhanced
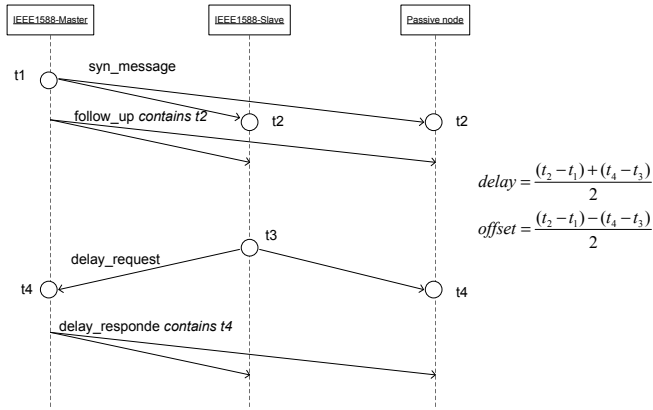

Fig. 7.   IEEE - PBS synchronization

version of [17] for broadcast, single hop communications, named IEEE 1588-PBS (Pairwise Broadcast Synchronization). The main objective of this protocol consists in reducing the synchronization phase overhead and minimizing the energy consumption, while achieving a precision degree about 200 nanoseconds.

IEEE 1588-PBS is based on one time master to perform the synchronization mechanism; and one active slave to receive the synchronization message and to send the request to the master. The other nodes are passive nodes which listen to the exchanged data between the master and the active slave to

estimate the current time. The figure 7 illustrates the IEEE 1588-PBS mechanism. It is worth to note the high availability of this mechanism, since if the active node fails one of the passive nodes can be elected to perform synchronization.

Hence, because of its high precision, good availability and reduced overhead, the IEEE1588-PBS is considered as an interesting candidate for time-critical avionics applications to guarantee the accuracy of TDMA implementation.

C. Reliability Mechanisms

For safety-critical avionics network, the probability of failure should be less than 10^{-9} per flight hour. This condition could be easily guaranteed with the current wired avionics network. However, with wireless technology, the task seems more complicated due to erroneous propagation environment and interference. At the beginning phase, to cope with this limitation, we propose two possible solutions to decrease the probability of errors and failure by replacing the partial backbone network. Because the AN's backbone includes a primary network and some back-up networks, there are two possibilies for the replacement. The first solution is based on keeping a wired backup network for the proposed WAN; whereas the second consists in using the proposed WAN to replace the current backup network for avionics network. We believe that the two solutions are feasible and the wiring reduction should be compared in the two cases.

Furthermore, in order to guarantee reliable communications for safety-critical avionics, adequate acknowledgment and retransmission mechanisms are required. Since the communication pattern for avionics applications is multicast, an enhanced mechanism is needed to avoid the collisions between the acknowledgment messages sent by different receivers and to reduce the overhead.
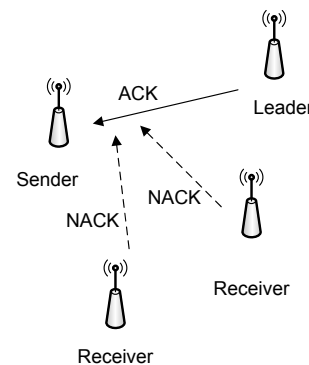

Fig. 8.   A multicast reliable transmission

In this specific area, in [19], the authors propose an enhanced acknowledgment mechanism for multicast communications. This approach consists in selecting one of the receivers as a "leader" to send a feedback to the sender. If the packet is correctly received then the leader will send a positive acknowledgement (ACK) to the sender, else there is no feedback from the leader. However, in case of erroneous transmission for the other receivers, they will reply with Negative ACKs.

Consequently, these NACKs will collide with the ACK message sent by the leader, which will prompt the retransmission from the sender. Finally, when the sender receives NACK or the time out occurs, the packet is immediately retransmitted to all the receivers. This approach is illustrated in figure 8.

Hence, this mechanism could be implemented for safety critical avionics network to guarantee reliable multicast communications, while reducing overhead and increasing efficiency.

V. CONCLUSION AND FUTURE WORK

The opportunities and challenges for using wireless interconnect for safety-critical avionics have been discussed in this paper. The benefits of such an implementation include weight reduction, increased flexibility and decreased costs and maintenance. However, electromagnetic susceptibility and security still are the main challenges to handle.

The most common wireless technologies have been investigated under the hard avionics requirements to explore the "Fly-By-Wireless" feasibility. ECMA-368 is introduced as the most suitable COTS technology to use in terms of timeliness, reliability and capability of limiting sensitivity to interferences.

A Wireless Avionics Network (WAN) has been proposed based on hybrid architecture UWB/ Switched Ethernet to minimize communication latencies, reduce electromagnetic susceptibility and increase scalability. Communication predictability is enhanced due to TDMA-based protocol to guarantee a contention-free access. Furthermore, reliability mechanisms adequate to multicast communications are integrated to reduce overhead and guarantee reliable communications. The security risks like "man-in-the-middle" attacks are inherently reduced because of the low emission power and short range communications with UWB technology.

REFERENCES

[1] A. E. E. Committee, "Aircraft Data Network Part 7, Avionics Full Duplex Switched Ethernet (AFDX) Network, ARINC Specification 664." Annapolis, Maryland: Aeronautical Radio, 2002.

[2] Avionic Systems Standardisation Committee, "Guide to avionics data buses," 1995.

[3] R. B. GmbH, "CAN specification Version 2,0," 1991.

[4] C. Furse and R. Haupt, "Down to the wire," *Spectrum, IEEE*, vol. 38, no. 2, pp. 34–39, 2001.

[5] P. Suriyachai, J. Brown, and U. Roedig, "Time-critical data delivery in wireless sensor networks," *Distributed Computing in Sensor Systems*, pp. 216–229, 2010.

[6] A. Willig, K. Matheus, and A. Wolisz, "Wireless Technology in Industrial Networks." Proceedings of the IEEE, 2005.

[7] T. Coelho, R. Macedo, and et al., "A fly-by-wireless UAV platform based on a flexible and distributed system architecture." IEEE International Conference on Industrial Technology, 2006.

[8] A. Akl, T. Gayraud, and P. Berthou, "Investigating Several Wireless Technologies to Build a Heterogeneous Network for the In-Flight Entertainment System inside an Aircraft Cabin." Washington, DC, USA: The 6th International Conference on Wireless and Mobile Communications, 2010.

[9] F. Leipold, D. Tassetto, and S. Bovelli, "Wireless in-cabin communication for aircraft infrastructure," *Telecommunication Systems*, pp. 1–22, 2011.

[10] R. Yedavalli and R. Belapurkar, "Application of wireless sensor networks to aircraft control and health management systems," *Journal of Control Theory and Applications*, vol. 9, no. 1, pp. 28–33, 2011.

[11] N. Thanthry and R. Pendse, "Aviation data networks: Security issues and network architecture." International Carnahan Conference on Security Technology, 2004.

[12] O. Elgezabal Gomez, "Fly-by-wireless: Benefits, risks and technical challenges." Fly by Wireless Workshop (FBW), 2010.

[13] T. Paul and T. Ogunfunmi, "Wireless LAN comes of age: Understanding the IEEE 802.11 n amendment," *Circuits and Systems Magazine, IEEE*, vol. 8, no. 1, pp. 28–54, 2008.

[14] W. Alliance, "Ecma-368 high rate ultra wideband phy and mac standard," *ECMA Std.*, 2008.

[15] S. Yong, P. Xia, and A. Valdes-Garcia, *60GHz Technology for Gbps WLAN and WPAN: From Theory to Practice.* Wiley, 2011.

[16] K. Lee and J. Eidson, "IEEE-1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems." In 34th Annual Precise Time and Time Interval (PTTI) Meeting, 2002.

[17] H. Cho, J. Jung, and et al., "Precision time synchronization using ieee 1588 for wireless sensor networks." The International Conference on Computational Science and Engineering, 2009.

[18] R. Albu, Y. Labit, and et al., "An energy-efficient clock synchronization protocol for Wireless Sensor Networks." Wireless Days, 2010.

[19] J. Kuri and S. Kasera, "Reliable multicast in multi-access wireless LANs," *Wireless Networks*, vol. 7, no. 4, 2001.